PCT/GB 2003 / 0 0 5 6 3 2

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed J Evans.

Dated 21 January 2004

Patents Form 1/77

The Patent Office

Patents Act 1977
(Rule 16)

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

1. Your reference RJ/GM/N13281

2. Patent application number *(The Patent Office will fill this part)* 20 DEC 2002 0229759.6

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

BECRYPT LIMITED
Wyvols Court
Swallowfield
Berkshire RG7 1WY

08531717001

Patents ADP number *(if you know it)*

If the applicant is a corporate body, give the country/state of its incorporation United Kingdom

4. Title of the invention
SECURITY DEVICE

5. Name of your agent *(if you have one)*
"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

Williams Powell
4 St. Paul's Churchyard
London
EC4M 8AY

Patents ADP number *(if you know it)* 5830310001 ✓

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority appliation number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earleir UK application, give the number and the filing date of the earlier application.

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(answer 'Yes if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d))

YES

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	10
Claim(*s*)	
Abstract	
Drawing(*s*)	3

10. If you are filing one of the following, state how many against each item.

Priority documents

translations of priority documents

Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*

Request for preliminary examination and search *(Patents Form 9/77)*

Request for substantive examination *(Patents Form 10/77)*

Any other documents *(please specify)*

11. I/we quest the grant of a patent on the basis of this application.

Signature

Date 20/12/02

12. Name and daytime telephone number of person to contact in the United Kingdom

Mr Lee Anderson 020 7329 4400

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you form applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

*a) **If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.***

b) Write your answers in capital letters using black ink or you may type them.

c) If there is not enough space for all the relevant details on any part of this form, please continue on a sepate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.

d) If you have answered 'Yes' Patents Form 7/77 will need to be filed.

e) Once you have filled in the form you must remember to sign and date it.

f) For details of the fee and ways to pay please contact the Patent Office.

SECURITY DEVICE

The present invention relates to a security device for securing electronic equipment having a memory, such as a personal computer, personal digital assistant (PDA), mobile telephone and the like.

A problem with many portable devices of such a nature is that they have limitations in terms of processing power and of the software provided to operate them. Yet, these devices often store sensitive information which requires protection. In fact, many such devices, in particular portable digital assistants, fail to achieve baseline certification, for example by the Communications & Electronics Security Group (CESG) of GCHQ (Government Communications Head Quarters).

The present invention seeks to provide a security system for such apparatus.

According to an aspect of the present invention, there is provided a security system for protecting data stored in a memory of an electronic device and provided with a memory management unit and an operating system, including means operable to interact directly with the memory management unit to control access to the memory management unit by the operating system.

Advantageously, the security system is operable to control access control data of the memory management unit.

In the preferred embodiment, the security device includes a hidden memory section within the device's memory not accessible by the device's operating system. The hidden memory section provides hidden storage space for functions of the security system.

The security system preferably provides for encryption of data stored in the memory.

According to another aspect of the present invention, there is provided a method of protecting data stored in a memory of an electronic device and provided with a memory management unit and an operating system, including the step of interacting directly with

the memory management unit to control access to the memory management unit by the operating system.

One embodiment implements a filter driver referred to herein as the encrypting driver. The encrypting driver implements a strategy for the protection of the encryption key used for data encryption.

The principal features of the preferred embodiments are that the system hides memory from the operating system, which is achieved by interacting directly with the memory management unit (MMU). The system applies access control to acquired memory. Whilst access control might not be achieved through the operating system directly, MMU access control data may be accessed and modified such that memory becomes unavailable to the system.

The preferred embodiments can provide a security product for mobile computing devices such as personal digital assistants (PDAs), mobile telephones and personal computers, and in particular a comprehensive set of security features, including an encryption component for the transparent encryption of all data stored on removable memory cards (SD/Compact Flash cards). The preferred embodiments seek to achieve baseline certification by the Communications & Electronics Security Group (CESG) of GCHQ (Government Communications Head Quarters).

One embodiment of system is designed for use by devices operated by the Windows CE® operating system.

With protection provided with Windows CE, all physical memory pages are accessible to kernel code or device drivers running with system privileges. Thus, under normal operation, potentially rogue or malicious code can interfere with key material wherever placed. The operating system does not provide the facility to modify this behavior.

The software configuration of a PDA device, for example, is dependent upon the contents of a system database referred to as the registry. Unlike the registry used on desktop operating systems, the Windows CE® registry does not support access control security. Any application on the PDA can access and modify registry settings on PDA's running Windows CE®.

The preferred embodiments implement a mechanism whereby the values of registry settings can be enforced such that they cannot be modified by other applications. This is enforced by:

a) maintaining an internal representation of the correct values of specific registry entries;

b) regularly monitoring registry contents; and

c) resetting registry entries where incorrect values are detected.

The security provided by registry enforcing functionality results from the fact that the functionality is implemented within the encryption driver, which interacts directly with the MMU. The driver would be difficult for a rogue application to stop (unload). Furthermore, unloading the driver would cause the system to enter an unstable state.

Embodiments of the present invention are described below, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 shows an example of electronic device and an embodiment of security system, in which a hidden memory section is created;

Figure 2 shows an operational view of the system of Figure 1 in which access to look-aside buffers has been modified by the security system;

Figure 3 shows an operational view of the system of Figures 1 and 2 in which the processor is switched to a supervisor mode;

Figure 4 shows an embodiment of filter-driver encryption for the security system;

Figure 5 shows an embodiment of virtual to physical address translation.

The main embodiment described below is described in relation to an electronic device which uses the Windows CE® operating system. However, the security system disclosed herein is independent of operating system so could be applied to electronic devices which use different operating systems. Prior to describing this embodiment, there is described an overview of the system.

In broad terms, the preferred embodiments provide a mechanism for the protection of encryption key material within microprocessor-based cryptographic systems. Protection of key material is a central concern in the design of systems that attempt to protect data through the process of data encryption. Where hardware platforms employ standard operating systems, the level of security achievable by a software-based cryptographic module is limited by the security-related characteristics of the operating system. The mechanism outlined below, allows a level of security to be achieved that is dependent upon characteristics of the hardware platform, thereby providing a level of independence from operating system characteristics.

The preferred encryption key protection mechanism consists of a number of distinct phases, these entail:

1) the acquisition of physical memory;
2) the location of references to the acquired physical memory as maintained by hardware components; and
3) controlling access to acquired physical memory for the exclusive use of encryption.

Referring to Figure 1, key protection requires the acquisition of a section 12 of memory 10 from the operating system 14 of the electronic device to be protected. The memory section 12 is used for the storage of the data encryption key. The details of the process of memory acquisition is dependent upon the operating system and is therefore not

expanded upon here as it will be readily apparent to the skilled person. The result of memory acquisition is the removal of a specific section 12 of physical memory 10 from that regarded as available by the operating system 14. Whilst the security of the key protection mechanism is not dependent upon the details of memory acquisition, the stability of the operating system is, and should therefore be, considered during the implementation of a memory acquisition scheme.

Referring now also to Figure 2, the key protection mechanism is dependent upon the existence of a hardware module referred to as a memory management unit (MMU) 16. MMUs are common within microprocessor-based systems, and support the common use of virtual memory mapping whereby physical memory addresses are mapped to virtual addresses used by the operating system and software applications. The MMU 16 is responsible for managing the system's memory and contains details of physical to virtual memory mapping, memory cache and buffering, and access control information. An operating system 14 is required to initialise an MMU 16 to contain a memory configuration as required by the operating system, following which the MMU 16 maintains configuration data, and interacts directly with the microprocessor 18 during memory read and write operations.

MMU configuration data referred to as MMU look-up tables are created within the system's physical memory 10, and maintained internally to the MMU 16 within translation look-aside buffers (TLBs) 20. TLBs 20 create a cached copy of look-up tables for the purpose of fast memory access.

This embodiment includes a software component, referred to here as the key protection module (KPM) 22. The key protection module 22 requires operating system privileges that allow direct access to the physical memory 14. This is typically achieved by implementing a kernel-mode application or driver. The key protection module 22 is required to locate within the MMU look-up tables the entries relating to the memory section acquired as outline above.

Referring now also to Figure 3, the key protection module 22 modifies access control information within MMU look-up tables such that memory containing the encryption key is only accessible during cryptographic activity initiated by the driver.

The key protection module 22 undertakes a series of write operations to the physical memory 10 containing access control information within MMU look-up tables relating to the acquired memory section. The key protection module 22 then triggers the MMU 16 to update look-aside buffer 20 contents. Any subsequent read or write operations performed by the operating system or applications running under the operating system will fail.

To protect its own access to key data, the key protection module 22 KPM utilises microprocessor support of separate processor modes. A processor mode separate to that used for user-applications should employ a separate data stack, and allow code execution that cannot be pre-empted by other processes. This mode is referred to here as supervisor-mode.

The key protection module 22 executes a sequence of processor instructions to place the processor 18 in supervisor-mode prior to cryptographic activity. The key protection module 22 then performs write operations to the corresponding look-up table entry to allow access to key data. Cryptographic routines are completed; following which access control to key data is re-applied through the look-up tables.

The key protection module 22 flushes any sensitive data held on the stack following cryptographic activity.

The following description relates to an embodiment devices for use in a personal digital assistant (PDA) using Windows CE® as its operating system.

Referring to Figure 4, a number of high-level requirements were identified for the provision of PDA encryption such that security assurances could be achieved suitable for certification. The general preferred features may be summarised as:

a) the product should be transparent to the user during normal product use;

b) the product should encrypt all data on all removable memory cards;

c) encryption should be performed with an algorithm and key length appropriate for UK restricted material;

d) mechanisms should be implemented for the protection of key material;

e) encryption overhead should be minimized; and

f) the product should be easy to install.

The wish for transparency and the encryption of all data (as opposed to the more common virtual-drive approach) is achieved by the development of filter drivers to filter all data written to and read from memory cards 30.

The filter device drivers (shims) 32 intercept all read and write operations made to the memory card device-drivers provided with the PDA. The approach taken is for the shims to communicate with a separate device driver 34 for cryptographic activity as shown in Figure 4.

The use of a shim allows the general requirements a) and b) to be met, while the remaining requirements are addressed through the architecture of the separate driver, referred to as BC driver 36.

Encryption algorithm options for baseline can include 3DES (Data Encryption Standard), AES (Advanced Encryption Standard) and a CESG proprietary algorithm. AES might be preferred for its performance advantages and its applicability to the commercial sector. A 128-bit key is deemed appropriate for baseline certification.

The principal technical challenge identified by CESG relates to requirement d). This involves providing sufficient control and protection of the encryption key. The requirement provides a significant challenge in a pocket PC (Windows CE®) environment due to the memory architecture adopted. Additionally, the operating system lacks the security architecture common to the Windows NT/2000® operating systems. The embodiments described herein address these issues.

Referring now also to Figure 5, the system provides protection of an installed encryption key by acquiring a section 12 of device memory 10 and applying protection to the memory 10 such that other applications 38 cannot access the memory 10 either through malicious or accidental activity.

Memory management is the ability to manage the system address space. A memory-managed address space as seen by a program running under Windows CE is referred to as a virtual address space 42. A virtual address is then translated by the system into a physical address 46 prior to accessing memory.

Memory management provides address translation and provides a persistent state following a faulting (uncompleted) memory access. Additionally, the MMU 16 will provide access control functionality made use of by the operating system 14.

Address translation is performed using page tables, which can involve multiple steps, dependent upon the granularity of the translated page size. A single-level lookup is illustrated in Figure 5 (for a two level look-up example).

A translation base value is combined with the first-level index to provide the address of a page table entry (PTE) 44. This entry then provides the physical base, which is concatenated with the physical address index to provide the required physical address 46. Additional fields within the page table entry 44 contain access control information for the MMU model.

To enhance system performance, the processor 18 implements a cache of address mapping entries in translation look-aside buffer 20.

Access to the physical memory 10 is achieved by locating the data structures created by the operating system 14 during the initialisation of the MMU 16. The system modifies the VA (42) => PA (46) mappings, and removes a physical address 46 entry from a list maintained by the operating system 14, effectively reducing the memory that the system 'believes' is available.

This provides a memory area reserved for use by the system. However, it remains possible that a rogue or malicious application could locate the physical page and tamper or copy the key. The system therefore implements protection of the memory area as described below.

To provide protection of the product encryption key, the BC Driver 36 will modify the MMU tables so that the physical memory 10 holding the AES keys is protected from access. Through access to MMU registers sections and pages for both privileged and non-privileged program execution can be protected using access permissions (AP bits), allowing no_access, read_only, or read_write permissions for supervisor and user modes. This is achieved by initialising a section of the MMU tables described above so that AES key memory is rendered not accessible by any code. When access to the round keys in needed by the AES algorithm implemented by the system, the MMU tables will be modified to allow access to the keys.

This presents a second problem, as processes within a multi-tasking environment may normally be "pre-empted" such that they are placed in a suspended state, allowing another process to execute.

Encryption is required to be performed in a non pre-emptive manner. This is achieved thrugh access to processor registers to perform a switch to supervisor mode, call the required function and return to the system mode in which the driver normally runs. The system therefore implements a assembly language routine to achieve this effect from within the driver.

Figure 6 shows an example of user interface for requiring the input of a user password to allow for decryption of encrypted data. The interface provides for access only by entry of the correct password 50, requirement to provide another password for modifying the system set up 52 and for the installation or modification of PDA settings, configuring of desktop settings and the assistance of PDA password recovery 54, using mechanisms and procedures known in the art.

The embodiments described provide an encryption product that address a number of vulnerabilities inherent in operating systems used in a number of electronic devices. They can provide transparent encryption with sufficient control over key material, by exploiting the memory management model employed by processor of such devices.

The embodiments described herein can provide a high level of security assurance, a system which is transparent to the user and which can support remote deployment and configuration. They can therefore offer a simple way of providing good security protection for data on lost or stolen computers and other electronic devices. Authentication preferably occurs at boot time using password hashing with the option of secondary authentication (be it by way of second code or additional component.

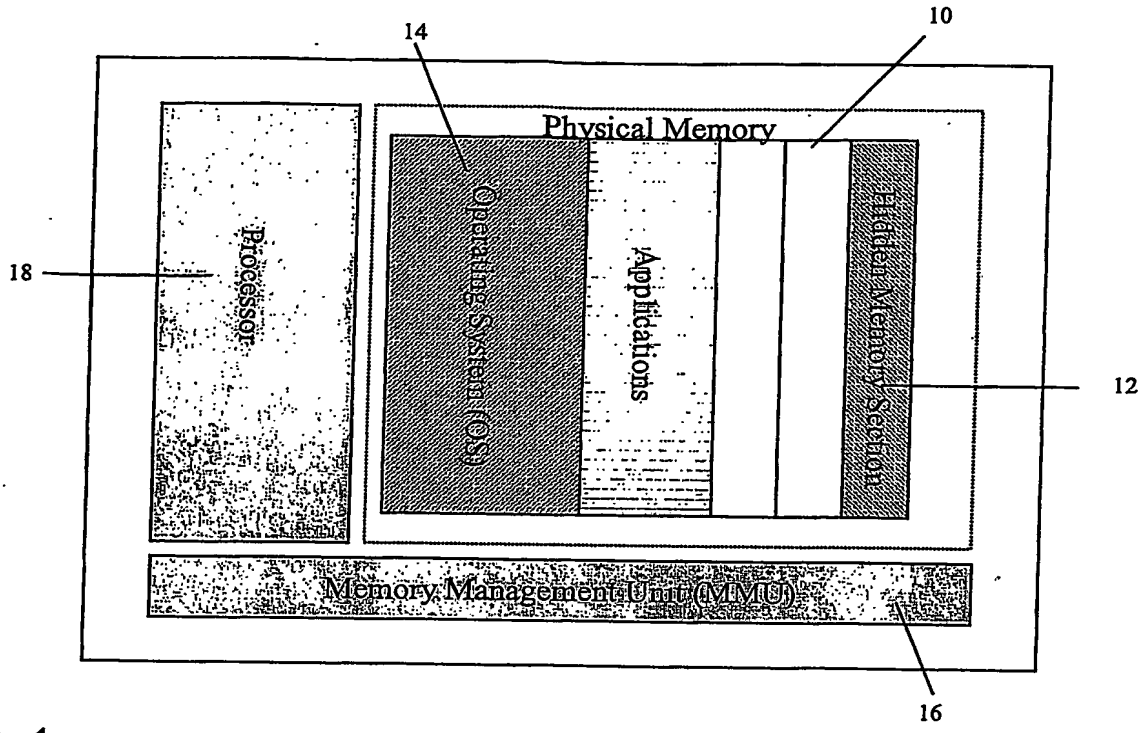

14
10
Physical Memory
Processor
Operating System (OS)
Applications
Hidden Memory Section
18
12
Memory Management Unit (MMU)
16

FIG. 1

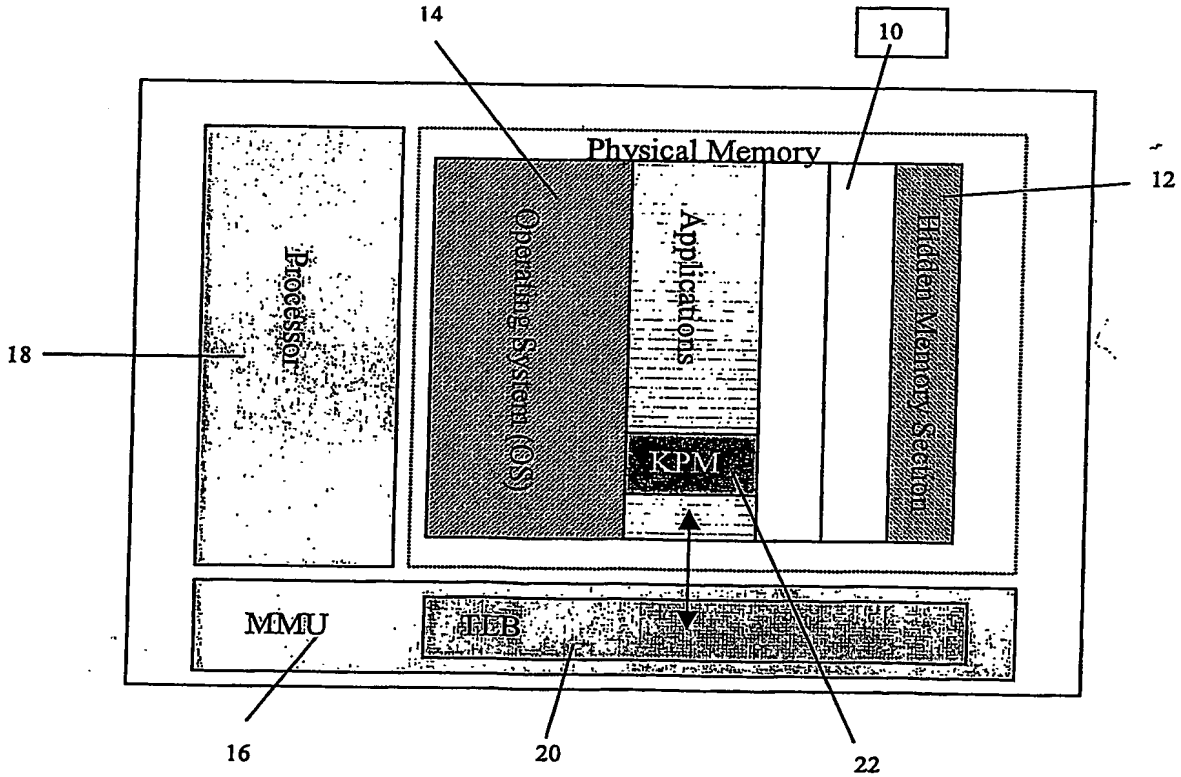

14
10
Physical Memory
12
Processor
Operating System (OS)
Applications
Hidden Memory Section
18
KPM
MMU
TLB
16
20
22

FIG. 2

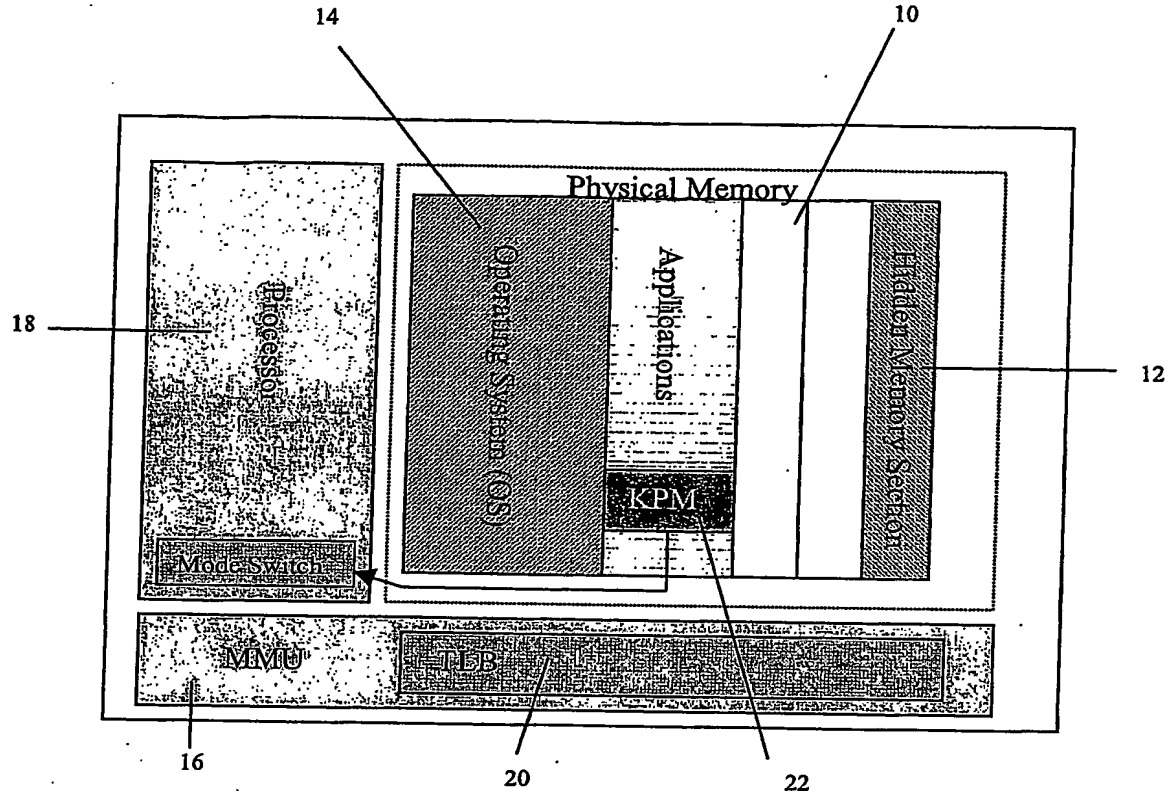
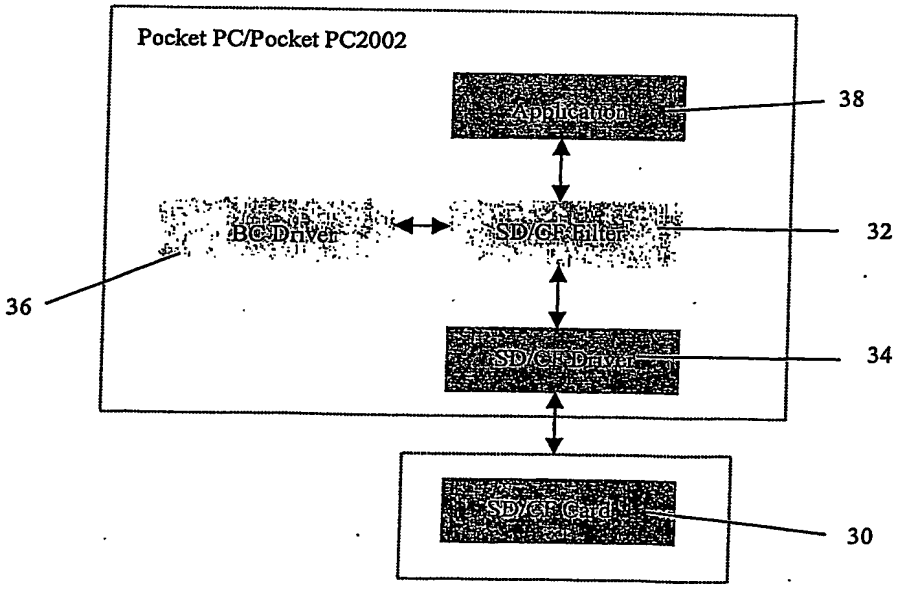

14
10
Physical Memory
Operating System (OS)
Applications
KPM
Hidden Memory Section
12
18
Processor
Mode Switch
MMU
TLB
16
20
22

FIG. 3


Pocket PC/Pocket PC2002
Application
38
BC Driver
SD/CF Filter
32
36
SD/CF Driver
34
SD/CF Card
30

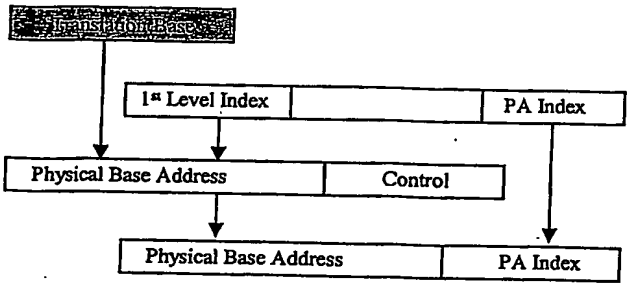

Translation Base
1st Level Index
PA Index
Physical Base Address
Control
Physical Base Address
PA Index
MMU Register 40
Virtual Address 42
PTE 44
Physical Address 46

FIG. 5

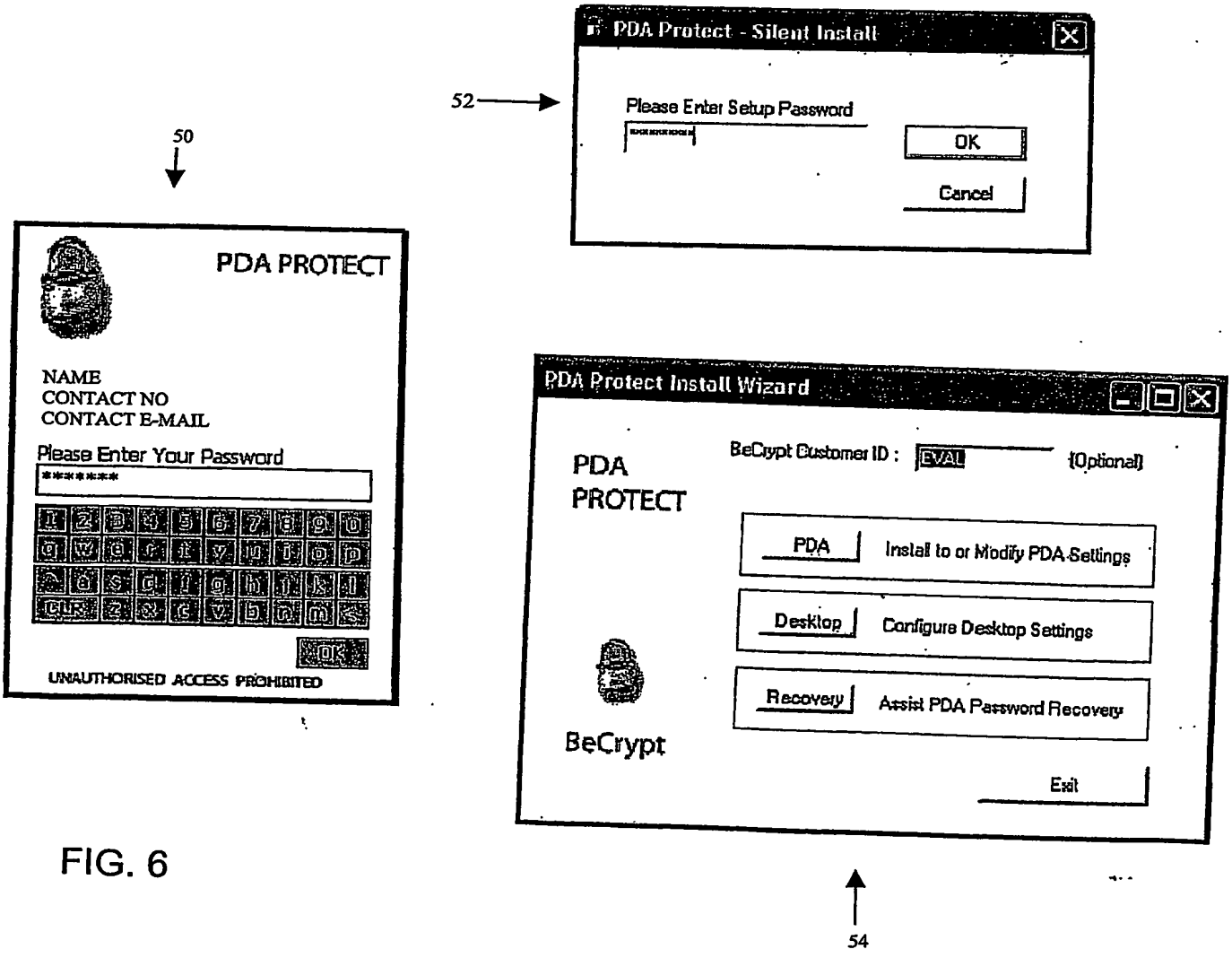

50
52
PDA Protect - Silent Install
Please Enter Setup Password
OK
Cancel
PDA PROTECT
NAME
CONTACT NO
CONTACT E-MAIL
Please Enter Your Password
UNAUTHORISED ACCESS PROHIBITED
PDA Protect Install Wizard
PDA PROTECT
BeCrypt Customer ID : EVAL (Optional)
PDA
Install to or Modify PDA Settings
Desktop
Configure Desktop Settings
Recovery
Assist PDA Password Recovery
BeCrypt
Exit
54

FIG. 6

PCT Application
GB0305632